METHOD FOR GENERATING AN ENCRYPTION KEY

Abstract

A method for generating an encryption key wherein combinations of a host identification and a content identification are concatenated to produce the encryption key. The content identification is unique to each block of plaintext to be transmitted over an unsecured interface to a storage device. The content identification is appended to the resulting ciphertext for transmission to the storage device. The ciphertext is retrieved by the host device wherein the host identification and appended content identification are used to recreate the encryption key and thus decrypt the ciphertext. Also using a time variable to generate the encryption key provides a method for limiting the duration during which the ciphertext can be decrypted.